CLAIMS

1. A method of obtaining security and audit ability in an on-line system, the method comprising the steps of:

- generating a random number by means of a random number generator,
- providing a sequence number for each of the random numbers generated so as to create a random number - sequence number pair,
- storing the created random number - sequence number pair in a storage means,

the method further comprising the step of, at a chosen time, verifying stored random number - sequence number pairs, so as to ensure that every stored random number - sequence number pair is an authentic random number - sequence number pair.

2. A method according to claim 1, wherein the verifying step is performed at at least substantially equal time intervals.

3. A method according to claim 1 or 2, wherein the generated random number is a true random number, the random number generator being a true random number generator.

4. A method according to any of claims 1-3, wherein the storing step is performed by storing the random number - sequence number pair in a storage means with limited access.

5. A method according to any of claims 1-4, wherein the random number generator has limited access.

6. A method according to claim 4 or 5, wherein access to the limited access area(s) can only be obtained by one or more authorised persons.

7. A method according to claim 6, wherein access to the limited access area(s) can only be obtained by two or more authorised persons.

8. A method according to claim 7, wherein the two or more authorised persons each represents an authority, so that at least two authorities are represented when access to the limited access area(s) is obtained.

9. A method according to claim 8, wherein at least one of the authorised persons represents an operator, and at least one of the authorised persons represents an auditor.

10. A method according to claims 1-9, wherein the limited access area further generates a transaction log comprising:

- a timestamp,
- a game-id,
- a customer-id,
- a sequence number, and
- a random number,

wherein the transaction log is stored in a second limited access area.

11. A method according to claims 1-10, wherein the limited access area further comprises a prize table.

12. A method according to claims 1-11, wherein the second limited access area can only be accessed by one or more authorized persons.

13. A method according to claims 1-12, wherein the transaction log further comprises a prize category and a prize amount.

14. A method according to claims 1-13, wherein the transaction log is used to audit transactions in an online system by one or more audit processes performed by audit processing means.

15. A method according to any of claims 1-14, further comprising the step of issuing a ticket comprising information relating to the sequence number.

16. A method according to claim 15, wherein the on-line system is a lottery, and the issued ticket is a lottery ticket.

17. A method according to claim 16, wherein the ticket further comprises information relating to a winning/no winning category of the ticket.

18. A method according to claim 16 or 17, wherein the step of issuing a ticket is based upon the random number and a probability table, the method further comprising the step of updating the probability table in response to the issued ticket, so as to maintain an at least substantially fixed winning/no winning ratio.

19. A method according to claims 1-18, wherein the information regarding the on-line ticket is stored in an evidence storage means.

20. A method according to claims 1-19, wherein the online ticket information in the evidence storage means is used to audit transactions in a online system by one or more of the audit processes performed by audit processing means.

21. A method according to any of claims 1-20, wherein the on-line system is a code generation system.

22. A method according to any of claims 1-21, wherein the on-line system is an encryption system.

23. A method according to any of claims 1-22, wherein the on-line system is a money transfer system.

24. A method according to any of claims 1-23, further comprising the step of alerting an operator in case the verifying step results in the discovery of one or more non-authentic random number - sequence number pairs.

25. A method according to any of claims 1-24, wherein the step of generating a random number is performed upon the request from a user.

26. A method according to any of claims 1-25, further comprising the step of receiving payment from a user.

27. A method according to any of claims 1-26, wherein the verifying step comprises checking that a certain number of random numbers has been generated.

28. A method according to any of claims 1-27, wherein the verifying step comprises the steps of:

- checking whether a given random number - sequence number pair has previously been stored in the storage means,
- marking said given random number - sequence number pair as a true pair in case it has previously been stored in the storage means, and
- alerting an operator in case the given random number - sequence number pair has not previously been stored in the storage means.

29. A secure and auditable on-line system comprising:

- a random number generator,
- means for providing a sequence number for each generated random number, so as to create a random number - sequence number pair,
- storage means for storing the created random number - sequence number pair,
- verifying means for verifying, at a chosen time, stored random number - sequence number pairs against a transaction created in the online system, so as to ensure that every stored random number - sequence number pair is an authentic random number - sequence number pair.

30. An on-line system according to claim 29, wherein the verifying means is adapted to perform verification at at least substantially equal time intervals.

31. An on-line system according to claim 29 or 30, wherein the random number generator is a true random number generator.

32. An on-line system according to any of claims 29-31, wherein the storage means has limited access.

33. An on-line system according to any of claims 29-32, wherein the random number generator has limited access.

34. An on-line system according to claim 32 or 33, wherein access to the limited access area(s) can only be obtained by one or more authorised persons.

35. An on-line system according to claim 24, wherein access to the limited access area(s) can only be obtained by two or more authorised persons.

36. An on-line system according to claim 25, wherein the two or more authorised persons each represents an authority, so that at least two authorities are represented when access to the limited access area(s) is obtained.

37. An on-line system according to claim 36, wherein at least one of the authorised persons represents an operator, and at least one of the authorised persons represents an auditor.

38. An on-line system according to claims 29-37, wherein the first storage means further comprises means for generating a transaction log and a get list.

39. An on-line system according to claims 29-38, wherein the transaction log is stored in a second storage means.

40. An on-line system according to claims 29-39, wherein the second storage means is an evidence storage means.

41. An on-line system according to claims 29-40, wherein the data stored in the first storage means is used to audit transactions in a online system by an audit processing means.

42. An on-line system according to claims 29-41, wherein the data stored in the evidence storage means can be used to audit transactions in a online system by an audit processing means.

43. An on-line system according to claims 29-42, wherein the first storage means, second storage means and the audit processing means are concealed in a certification zone.

44. An on-line system according to claims 29-43, wherein the evidence storage means can only be obtained by one or more authorized persons.

45. An on-line system according to claims 29-44, wherein the storage means further comprises means for generating and maintaining a prize table.

46. An on-line system according to any of claims 29-45, further comprising means for issuing a ticket comprising information relating to the sequence number.

47. An on-line system according to claim 46, wherein the on-line system is a lottery, and the issued ticket is a lottery ticket.

48. An on-line system according to claim 47, wherein the ticket further comprises information relating to a winning/no winning category of the ticket.

49. An on-line system according to claim 47 or 48, wherein the ticket is issued based upon the random number and a probability table, the on-line system further comprising means for updating the probability table in response to the issued ticket, so as to maintain an at least substantially fixed winning/no winning ratio.

50. An on-line system according to any of claims 29-49, wherein the on-line system is a code generation system.

51. An on-line system according to any of claims 29-50, wherein the on-line system is an encryption system.

52. An on-line system according to any of claims 29-51, wherein the on-line system is a money transfer system.

53. An on-line system according to any of claims 29-52, further comprising means for alerting an operator and an auditor in case the verification results in the discovery of one or more non-authentic random number - sequence number pairs.

54. An on-line system according to any of claims 29-53, wherein the random number generator is adapted to provide a random number in response to a request from a user.

55 An on-line system according to any of claims 29-54, further comprising means for receiving payment from a user.

56. An on-line system according to any of claims 29-55, wherein the verifying means is adapted to checking that a certain random number in the online system is the same as in the evidence storage means within limited access area.

57. An on-line system according to any of claims 29-56, wherein the verifying means further comprises:

- means for checking whether a given random number - sequence number pair has previously been stored in the storage means,
- means for marking said given random number - sequence number pair as a true pair in case it has previously been stored in the storage means, and
- means for alerting an operator in case the given random number - sequence number pair has not previously been stored in the storage means.

58. A device for providing security and audit ability in an on-line system, the device comprising:

- a random number generator,
- means for providing a sequence number for each generated random number, so as to create a random number - sequence number pair,
- storage means for storing the created random number - sequence number pair,
- verifying means for verifying, at a chosen time, stored random number - sequence number pairs against a transaction created in the online system, so as to ensure that

every stored random number - sequence number pair is an authentic random number - sequence number pair,

the verifying means further comprising:

- means for checking whether a given random number - sequence number pair has previously been stored in the storage means,
- means for marking said given random number - sequence number pair in the online system as a true pair in case it has previously been verified against the random number – sequence number pair in the evidence storage means.
- means for alerting an operator in case the given random number - sequence number pair has not previously been verified,

wherein the storage means and the random number generator have limited access.

59. A computer program product for obtaining security and audit ability in an on-line system, the program being adapted to:

- generate a random number by means of a random number generator,
- provide a sequence number for each of the random numbers generated so as to create a random number - sequence number pair,
- store the created random number - sequence number pair in a first storage means,

the program further being adapted to verify stored random number - sequence number pairs, so as to ensure that every stored random number - sequence number pair is an authentic random number - sequence number pair.

60. The computer program product of claim 59, wherein a transaction log is generated, the transaction log comprising:

- a timestamp,
- a game-id,
- a customer-id,
- a sequence number, and
- a random number,

wherein the transaction log is stored in a second storage means..

61. The computer program product of claims 59-60, wherein the online generated information in a first storage means and a second storage means is used to audit

transactions in the online system by one or more audit processes performed by an audit processing means.